WACS高级用户手册

安腾网络

2005-06-01

1. 简介和特性....4
1.1. 版本信息....4
1.2. 内容简介....4
2. WACS安装....4
3. WACS配置....5
3.1. 连接....5
3.2. 管理权限....5
4. 命令详解....5
4.1.1. ?....5
4.1.2. acl....6
4.1.3. aclcfg....7
4.1.4. ap....7
4.1.5. arp....8
4.1.6. auth....9
4.1.7. backup....9
4.1.8. cfg....9
4.1.9. dhcp....10
4.1.10. enable....12
4.1.11. exit....12
4.1.12. filist....12
4.1.13. hostname....14
4.1.14. local....14
4.1.15. multi....15
4.1.16. nameserver....15
4.1.17. nat....16
4.1.18. no....17
4.1.19. ping....18
4.1.20. port....18
4.1.21. pppoe_c....19
4.1.22. proxyarp....20
4.1.23. radius....20
4.1.24. radsrv....22
4.1.25. reboot....22
4.1.26. route....22
4.1.27. servicename....23
4.1.28. set....23
4.1.29. session....24
4.1.30. show....26
4.1.31. snmp....26
4.1.32. src_route....27
4.1.33. tcplimit....28
4.1.34. telnet....28
4.1.35. telnetlist....29

4.1.36. time......29
4.1.37. upgrade......30
4.1.38. upgrade_lic......30
4.1.39. user......30
4.1.40. web......31
4.1.41. webp......31
4.1.42. webadm......33
4.1.43. wudb......34
4.1.44. write......35
5. 附件......35
5.1. dhcp umac文件格式......35
5.2. 用户数据文件格式......36
5.3. 如果正确升级版本......37
5.4. 如何获取新的License文件并进行更新......37
5.5. 为什么使用过程中会经常出现需要认证的页面？......38
5.6. 采用DHCP分配地址，为什么会出现地址冲突？......39
5.7. 设置ACL规则，怎么不起作用？......39
5.8. 管理页面不能打开，如何查看和对机器进行配置？......40
5.9. 机器重新启动后，不需要认证就可以上网？......40

1. 简介和特性

1.1. 版本信息

本手册对应的正式版本信息为：WAS AOS 1.3。如果您手上的设备为旧版本或者更新的版本，请查看与版本对应的手册，或者联系本地的技术支持。

1.2. 内容简介

本手册介绍了WACS的命令行操作内容，主要面向对象为：

1、通过命令行对设备进行配置的用户

2、对网络设备比较熟悉，想更多了解WACS设备的用户。

使用本手册，可以结合《WACS用户手册》对设备进行管理配置。

2. WACS 安装

- 首先，请确认 WACS 没有连接电源，而且电源是关闭的。

- WAN接口（E0口）的连接

  用10/100BaseT连接线连接出口。出口可以是ADSL路由器的LAN口、cable modem的LAN口或者是企业内部互联网的交换端口。

- LAN端口（E1口）的接入

  企业网的交换机或者HUB用直连线连接用户电脑连接到上,另一端连到WACS的E1端口上。如果想将WACS直接与PC或无线AP连接上，请使用交叉线。

- DMZ端口（E2口）的接入

  企业网的交换机或者HUB用直连线连接用户电脑连接到上,另一端连到WACS的E2端口上。如果想将WACS直接与PC或无线AP连接上，请使用交叉线。

- 打开电源
- 检查指示灯，当有网络设备接入 WACS 对应端口的指示灯会亮

3. WACS 配置

可以通过命令行方式对 WACS 设备进行配置。进行配置的电脑需要：

- 安装任何一种 Windows 操作系统
- 安装超级终端

3.1. 连接

配置 WACS 时，请将你的管理电脑用随机附带的串口线和 WACS 的 CONSOLE 口连接起来。然后打开超级终端，输入用户名和密码，登录到 WACS 的命令行管理界面中。

3.2. 管理权限

WACS 有两个管理用户，缺省设置为：

用户名：admin　密码：password

用户名：manager 密码：password

登陆成功后，进入到第一级管理界面。在此管理界面，只能查看配置，不能对设备配置进行修改。

如果需要对设备配置进行修改，输入 enable 命令：

was>　*enable*

系统将提示输入密码，输入密码（缺省为 eflow），进入配置界面。

4. 命令详解

4.1.1. ?

【用法】：?

【作用】：显示可用命令。

【例如】：

- was> ?

  enable get full right

  exit quit current shell

  ping test network

  show show system i

  time display or set system time

  ? show help

  显示当前命令模式下的可用命令。

4.1.2. acl

【用法】： acl deny/access block/pass/only

acl deny/access enable/disable/show

【作用】：第一条命令定义指定编号的 acl 规则的行为是阻止（block)、放行（pass)、只允许（only)。acl 规则是用来开展服务定制的(该功能必须和外接的 Radius server 相配合)，它定义了一组 IP 地址和该 acl 规则的行为。当用户进行认证时，选择了相应的服务名，那么该用户就只能根据相关联的 acl 规则进行访问。deny 和 access 分别对应两组地址。

第二条命令指定相应的 acl 规则是否开启和查看 acl 设置。

【例如】：

- wac # acl deny block
- was # acl deny enable
- was # acl deny show

  The ACL deny List

  Service:service1

  network address network netmask

  192.168.1.0 255.255.255.0

该命令显示了 acl deny 设定的 IP 地址范围是 192.168.1.0，该规则和服务 service1 相关联。当用户认证时选择的服务是 service1 时，该用户不能访问 192.168.1.0 子

网，但是可以访问其他子网。

【相关命令】：aclcfg

【注意事项】：

aclcfg 和 acl 是针对大运营商的方案而设计，需要和特定的设备配合才能使用。在 WACS 中不推荐使用此命令。

4.1.3. aclcfg

【用法】：aclcfg deny/access get/put tftp_server filename

【作用】：下载或者上传 acl 配置文件。

【例如】：

- was # aclcfg access get 192.168.0.168 acl0.txt

  将 acl 的 access 规则的配置文件 acl0.txt 从 TFTP Server 192.168.0.168 下载到 WACS。

- was # aclcfg access put 192.168.0.168 acl0.txt

  将 acl 的 access 规则的配置文件从 WACS 上传到 TFTP Server 192.168.0.168 并命名为 acl0.tx。

【相关命令】：acl，servicename

【注意事项】：

1、 aclcfg 文件的必须是 txt 文件，命名以能够表明 acl 相关内容为原则。

2、 aclcfg 文件的格式为：

    vod

    192.168.2.0 255.255.255.0

其中 vod 为服务名，192.168.2.0 255.255.255.0 是 vod 服务对应的 IP 地址。

3、 aclcfg 和 acl 是针对大运营商的方案而设计，需要和特定的设备配合才能使用。在 WACS 中不推荐使用此命令。

4、 acl 命令不是页面管理中的 ACL 规则，与页面的 ACL 规则对应的命令是 filist

4.1.4. ap

【用法】：ap global_key [key]

　　ap <ip> <key>

【作用】：管理需要进行认证的 AP。

- ap global_key [key]

配置全局使用的 radius KEY，所有 AP 都使用此 radius KEY

- ap <ip> <key>

配置某一 ap 的地址和使用的 KEY

【例如】：

- was> ap global_key key1

所有 AP 都可以使用的 Radius KEY 为 key1

- was> ap 192.168.1.111 key2

AP 的 IP 为 192.168.1.111，使用的 Radius KEY 为 key2

4.1.5. arp

【用法】：arp bind <ip> <mac>

arp unbind/query/del <ip>

arp show

【作用】：

- arp bind <ip> <mac>

  在 WACS 系统 ARP 表中增加一个固定的 IP 和 MAC 的绑定映射

- arp unbind/query/del <ip>

  解除 arp 的绑定、查询某个 ip 对应的 arp 表内容，删除某个 ip 对应的 arp 表内容

【例如】：

- was # arp bind 192.168.1.11 00:11:ca:10:1a:ac

  在系统 arp 表中增加 192.168.1.11 的固定绑定，对应的 mac 地址为 00:11:ca:10:1a:ac

- was # arp unbind 192.168.1.11

  解除 192.168.1.11 的 arp 绑定

- was # arp query 192.168.1.11

  查询 192.168.1.11 对应的 arp 表内容

- was # arp del 192.168.1.11

  在 arp 表中删除 192.168.1.11 的映射，如果 192.168.1.11 有绑定，不会从配置中删除，系

统重新启动后会继续起用绑定

4.1.6. auth

【用法】：auth chap/pap

【作用】：定义用户与外接 Radius 进行认证时的认证类型。

【例如】：

- was #　auth pap

  定义 was 用户与外接 Radius 认证时的认证类型为 pap。

- was #　auth chap

  定义 was 用户与外接 Radius 认证时认证类型为 chap。

4.1.7. backup

【用法】：backup

【作用】：备份系统当前 IOS 软件，当系统升级或者启动失败时可以使用备份的 IOS 软件进行启动或者工作。

【例如】：

- acs #　backup

将系统当前的 IOS 软件备份到内存中。

【注意事项】：

1、 WACS 升级版本时会先生成临时文件，不会因为升级一半未成功而造成系统损坏

2、 页面管理中没有备份操作系统的命令

4.1.8. cfg

【用法】：cfg put|get tftp_server　filename

　　　　cfg restore

【作用】：从 tftp 服务器获取或保存配置文件。

【例如】：

- was #cfg get 192.168.1.2 config.txt

从 tftp 服务器（地址为 192.168.1.2）中获取名字为 config.txt 的文件作为自己的配置文件。

注意：如果要使 config.txt 文件生效，你可以在下载完成该文件直接执行 reboot 命令，使系统重新启动后调用新的 config.txt 配置文件。

- was #cfg put 192.168.1.2 config.txt

  把当前系统的配置文件保存在地址为 192.168.1.2 的 tftp 服务器上，并命名为 config.txt。

- was #cfg restore

  将配置文件恢复成出厂配置。

4.1.9. dhcp

【用法】dhcp address <begin_ip> <num> <mask> <route>

dhcp umac enable/disable

dhcp umac list

dhcp umac get|put tftp_server filename

dhcp enet[1/2/3] input

dhcp lease <minute>

dhcp server enable|disable

【作用】：配置 DHCP 相关参数

- dhcp address <begin_ip> <num> <mask> <route>

  当 WACS 作为 DHCP Server 时，配置 DHCP 地址池中分配给用户的 IP 地址、掩码、网关等参数。Num 最大为 2550，不能超过此数，否则此命令不成功。

- dhcp umac enable/disable

  是否开启 IP 和 MAC 绑定功能。如果开启，则该 MAC 的用户只能分配指定的 IP 地址使用。

  注意：该功能的只能在二层网络环境中使用。

- dhcp umac list

  显示绑定的 IP 和 MAC 地址列表。

- dhcp umac get|put tftp_server filename

  下载或者上传用户 IP 和 MAC 绑定关系文件。

- dhcp enet[1/2/3] input

  设置端口的属性，如果设置端口为 input 属性，则该端口作为用户接入端口(此时该端口连接的用户必须进行认证才可以上网)，否则可以作为普通路由端口。当启用 DHCP Server 功能时，该端口的用户可以通过 dhcp 分配地址。

- dhcp lease <minute>

  设置 DHCP 协议分配 IP 地址的租期。

- dhcp server enable|disable

  开启或者关闭 WACS 的 DHCP Server 功能。

【例如】：

- was # dhcp address 10.1.1.2 253 255.255.255.0 10.1.1.1

  当 WACS 作为 DHCP Server 时，分配 10.1.1.2 开始的 253 个地址给用户，该子网的掩码是 255.255.255.0，用户网关地址为 10.1.1.1。

- was #dhcp umac enable

  激活 IP 和 MAC 绑定功能。

- was #dhcp umac list

  显示 IP 和 MAC 绑定表的内容。

- was #dhcp umac get 192.168.0.189 umac.txt

  从 192.168.0.189 的 TFTP Server 下载用户 IP 和 MAC 绑定关系的文件 umac.txt。其中当使用 put 命令时，上传当前用户的 IP 和 MAC 地址绑定关系文件到 TFTP Server 指定的目录下并命名为 umac.txt。

- was #dhcp enet1 input

  设置 enet1 口为用户接入端口，该端口连接的用户可使用 DHCP 协议进行地址分配，同时该端口连接的用户也必须进行认证才可以访问外网。

- was #dhcp lease 600

  设置 DHCP 分配的 IP 地址租期为 600 分钟。

- dhcp server enable

  WACS 启用 DHCP Server 功能。

【注意事项】：

1、 dhcp umac 命令在管理页面中没有，如果需要使用该功能，要在命令行进行配置

2、 dhcp umac 的文件格式定义见附件

【相关命令】：session

4.1.10. enable

【用法】：enable

【作用】：从普通模式进入到配置模式，需要输入超级密码。

【例如】：

- was> enable

  进入配置模式。

- was# enable passwd

  修改 enable 的密码，需要输入 2 次确认。

【注意】：为了保证系统的安全，建议用户修改默认的 enable 密码。

4.1.11. exit

【用法】：exit

【作用】：退出配置和监控。

【例如】：

- was# exit

  was>

  退出配置模式。

4.1.12. filist

【用法】：filist add/del port block/pass in/out protocol src [srcport scmp port] dst [dstport dcmp port] [quick]

filist flush/list

src_ip_pool 和 map_ip_pool 格式为 ip/prefix，其中 ip 为 ip 地址段，prefix 为地址中网络部分所占位数（十进制表示的掩码位数）。

【作用】：设置、清除或者显示报文过滤信息。

【参数说明】：

add/del　　增加/删除

port　　端口(例如 enet0， enet1 等）

block/pass　　阻塞/通过

in/out　　进入/输出（针对端口而言）

protocol　　针对的协议(icmp/udp/tcp)

src　　源地址(地址/掩码)

srcport scmp port (可选) 源端口

格式：srcport (‘>'‘<' ‘>=' ’'<=' ‘=') portnum

其中 srcport 是关键字，scmp 是以上的比较符号， portnum 是数字；

dst　　目的地址(地址/掩码)；

dstport dcmp port (可选) 目的端口，

格式：dstport (‘>'‘<' ‘>=' ’'<=' ‘=') portnum，

其中 dstport 是固定字，dcmp 是以上的比较符号， portnum 是数字；

quick (可选)找到规则后就直接返回，不再往下进行匹配。

【例如】：

- was# filist flush

  清除所有 filist 规则。

- was# filist list

  显示所有 filter 规则。

- was# filist add enet0 block out tcp 10.1.1.0/24 srcport > 1024 192.168.1.168/32 dstport = 23 quick

  在端口 enet0 上针对出去的 tcp 数据设置过滤规则,阻塞 源地址在 10.1.1.1 ～ 10.1.1.255 网段、源端口大于 1024，目的地址为 192.168.1.168、目的端口为 23 的数据包。在匹配该规则后，不再往下匹配。

- was# filist add enet0 pass out tcp 0.0.0.0/0 0.0.0.0/0

  在端口 enet0 针对出去的 tcp 数据设置过滤规则，让所有的数据通过。

- was# filist add enet0 pass out udp 0.0.0.0/0 0.0.0.0/0

  在端口 enet0 针对出去的 udp 数据设置过滤规则，让所有的数据通过。

- was# filist add enet0 pass out icmp 0.0.0.0/0 0.0.0.0/0

  在端口 enet0 针对出去的 icmp 数据设置过去规则，让所有的数据通过。

【注意事项】：

1、为了保证系统的安全，建议在现场调试时 block 掉 135，137，138，139，445，554，icmp 等端口和协议，防止病毒报文的传播。

4.1.13. hostname

【用法】：hostname <name>

【作用】：配置主机名。

【例如】：

➢ was# hostname wacs1

  wacs1#

定义主机名为 wacs1。

4.1.14. local

【用法】： local auth enable/disable

【作用】：配置是否进行本地认证，如果有外接的 Radius 服务器，不需要使用 WACS 自带数据库的帐号，则把本地认证取消。

【例如】：

➢ was# local auth enable

  允许本地认证。

➢ was# local auth disable

  禁止本地认证。

【参考命令】：radius

【注意事项】：

1、此命令在页面管理中没有

2、如果要使用本地 Radius，一定要允许本地认证，否则，认证将不会通过

3、即使打开了本地认证，也可以使用外接的 Radius Server，前提是用户帐号在本地数据库中不存在，WACS 优先查找本地数据库，如果没有用户信息，则自动转到外接的 Radius 服务器。

4.1.15. multi

【用法】：multi on/off

multi proxy ip port

multi show

【作用】：组播路由功能配置。

【例如】：

- was# multi on

  开启组播功能。

- was#multi proxy 224.1.1.1 23322

  配置 WACS 为组播组 224.1.1.1 的代理，端口号为 23322。

- was# multi show

  multi on

  multi proxy 224.1.1.2 23322

  显示组播配置的结果。

【注意事项】：

1、 此命令在管理页面中没有

2、 企业网很少用到组播，不推荐在 WACS 中使用此命令

4.1.16. nameserver

【用法】：nameserver primary/secondary <ip>

【作用】：配置 DNS 服务器。

【例如】：

- was# nameserver primary 192.168.1.2

  把第一域名服务器指向地址 192.168.1.2

- was# nameserver secondary 192.168.1.88

  把第二域名服务器指向地址 192.168.1.88

【注意事项】：

1、DNS 服务器的配置只有在用 dhcp 分配网络参数时有用。

4.1.17. nat

【用法】：nat add/del map/rdr <port> <src_ip_pool> [srcport port] <map_ip_pool> [dstport port] [portmap]

nat list/flush

src_ip_pool 和 map_ip_pool 格式为 ip/prefix，其中 ip 为子网地址，prefix 为地址中网络部分所占位数（即 10 进制表示的掩码长度）。

【作用】：配置地址转换表。该命令应该设置 port 参数之后进行设置。一般地，<port>参数是网络端口号（如 enet0，ppp0 等），src_ip_pool 是某个地址池中的一段地址。

map 是对源地址进行映射，改变数据包的源地址，对数据的目的地址不做任何改变,就是常说的动态 NAT。

rdr 是对目的地址进行改变，重新定向数据的目的地址，对数据的源地址不做任何改变（有的也称静态 NAT，或者反向 NAT）。

注意：使用rdr规则时，重定向的地址只能是一个，因此掩码都应该是 32。并且src_ip_pool地址应该是外部地址，<map_ip_pool>为内部地址。

【参数说明】：

add/del	增加/删除
map/rdr	映射/重定向
port	端口
src_ip_pool	源 ip 地址(ip/mask)
srcport port	(用于 **rdr** 规则，指定目的地址的端口，可选)
map_ip_pool	目的 ip 地址(ip/mask)
dstport port	(用于 **rdr** 规则，指定转向后的端口， 可选)
portmap	（用于 map 规则，可选）

【例如】:

- was# nat add map enet0 10.1.1.0/24 202.96.196.32/30

  在绑定了端口名字为 enet0 的上行接口上，将地址为 10.1.1.0 到 10.1.1.255 的地址转换为 202.96.196.32 到 202.96.196.35 的一段地址上。

- was# nat add rdr enet0 10.1.1.2/32 192.168.1.2/32

  在 enet0 端口上，把所有访问 10.1.1.2 的数据重定向到 192.168.1.2 上去。

- was# nat add rdr enet0 10.1.1.2/32 srcport 23 192.168.1.2/32 dstport 23

  在 enet0 端口上，把所有到 10.1.1.2 的 23 端口的数据重定向到 192.168.1.2 的 23 端口上。

- was#nat add map enet0 10.1.1.0/24 202.96.196.3/32 portmap

  在绑定了端口名字为 enet0 的接口上，将地址为 10.1.1.0 到 10.1.1.255 的地址转换到地址 202.96.196.3 上去，并在此地址上进行端口转换。

- was# nat del map enet0 10.1.1.0/24 202.96.196.32/30

  删除名字为“ enet0 的端口上，将地址为 10.1.1.0 到 10.1.1.255 的地址转换为 202.96.196.32 到 202.96.196.35 的一段地址 ”这样一条规则。

- was# nat list

  显示所有 nat 有效规则。

- was# nat flush

  删除所有 nat 规则和连接。

【注意事项】:

1、 nat 命令的 map 和 rdr 对应管理页面的 direct 和 redirect

4.1.18. no

【用法】：no servicename/snmp name

no port enet[0/1/2/3] vlan_id <num>

no dhcp address ip num

no dhcp enet[1/2/3] input

no session address ip num

no session ip

【作用】：

- no servicename/snmp name

  删除配置的服务名，删除 SNMP community 的参数。

- no port enet[0/1/2/3] vlan_id <num>

  去掉端口接收的指定 VLAN tag 配置。

- no dhcp address ip num

删除 DHCP 分配的指定地址段。

- no dhcp enet[1/2/3] input

  取消端口的接入端口属性。

- no session address ip num

  删除设置的允许接入的地址范围。

- no session ip

  强制指定 IP 地址的用户下线

【例如】：

- was# no servicename　serv1

  删除名字为 serv1 的服务。

- was#no snmp wacs

  删除名字为 wacs 的 snmp community。

- was#no session 10.1.2.23

  强制在线用户 10.1.2.23 下线。

【参考命令】servicename，snmp，session，dhcp，port

4.1.19.　ping

【用法】：ping　ip

【作用】：检测目标地址的连通性。在运行本命令之前，必须先配置好设备的接口地址或者地址池，并且要检查 filist 中是否禁用了 icmp 协议。

【例如】：

- was# ping 202.96.196.5

  检测目标地址为 202.96.196.5 的连通性。

【参考命令】：port，filist

4.1.20.　port

【用法】：port enet[0/1/2/3] ethernet <ip> <mask>

port enet0　pppoe_c

port enet[0/1/2/3] vlan_id <num>

port show

【作用】：配置通信端口封装类型和地址，以及 VLAN 配置，应该在配置过程的前期就使用此命令进行相关配置。如果改变了原来的端口配置，建议保存配置重新启动接入服务器。

【例如】：

- was#　port enet0 ethernet　192.168.1.10 255.255.255.0

  把端口 0 配置（一般作为上行端口）为以太封装类型，ip 地址为 192.168.1.10，掩码为 255.255.255.0。

- was#　port enet1 vlan_id 2

  配置端口 enet1 接收 vlan tag 为 2 的报文。

- was#　port enet0 pppoe_c

  配置端口 enet0 为 PPPoE 拨号封装模式。配合 PPPoE 帐号，WACS 会自动进行 PPPoE 拨号获取地址。

- port show

  检查端口配置。

【参考命令】：reboot，pppoe_c

4.1.21. pppoe_c

【用法】：pppoe_c　user　<name>　passwd　<passwd>

pppoe_c　start|stop

pppoe_c　show

【作用】：

- pppoe_c　user　<name>　passwd　<passwd>

  配置进行 PPPoE 拨号的用户帐号

- pppoe_c　start | stop

  启动 PPPoE 拨号或者停止 PPPoE 拨号

- pppoe_c　show

  显示 PPPoE 拨号信息

【例如】：

- was #　pppoe_c　user　adsl1　passwd　adsl1-password

定义 PPPoE 拨号的帐号为 adsl1，密码为 adsl1-password

- was #　pppoe_c　start

用定义的帐号进行 PPPoE 拨号

- was #　pppoe_c　stop

向 PPPoE 接入服务器申请断线

【参考命令】：port

4.1.22. proxyarp

【用法】：proxyarp add/del <ip> <mask>

proxyarp show

【作用】：代理一段 IP 地址的 ARP 应答。当 WACS 的 IP Pool 或者 NAT 的目标映射 IP Pool 是从本地子网（与上行以太网端口处于同一子网）再分配出来，而不是独立可路由的子网时，此时配合 nat add 命令而设置相应的 proxyarp。

【例如】：

本地管理网段为 202.104.87.208, mask 为 255.255.255.240。考虑用户的 IP 为 192.168.1.0/24，且把 202.104.87.212-215 四个 IP 地址用于 NAT 目标 IP Pool。此时的设置应该为：

- was#nat add map enet0 192.168.1.0/24 202.104.87.212/30 portmap(TCP,UDP 的端口映射)；
- was#nat add map enet0 192.168.1.0/24 202.104.87.212/30

  (非 TCP,UDP 的 NAT，可选)；
- was# proxyarp add 202.104.87.212 255.255.255.252

最后一条命令设置 WACS 接入服务器代理 202.104.87.212-215 四个 IP 地址的 ARP 应答。

4.1.23. radius

【用法】：radius [b]auth/[b]acct/dupacct ip <ip> key <key>

radius [b]auth/[b]acct/dupacct retry <num>

radius [b]auth/[b]acct/dupacct timeout <seconds>

radius [b]auth/[b]acct/dupacct port <port>

radius [b]auth/[b]acct/dupacct enable/disable

【作用】:配置远程拨入用户认证服务器和计费服务器。其中，bauth 是备份认证服务器、bacct 是备份计费服务器、dupacct 是对帐服务器。

【例如】:

- was#radius auth enable

  启用外接 radius 认证。

- was#radius auth ip 202.96.196.2 key password

  配置认证服务器 IP 地址为 202.96.196.2，通信密钥为 password。

- was#radius acct ip 202.96.196.2 key password

  配置计费服务器 IP 地址为 202.96.196.2，通信密钥为 password。

- was# radius auth timeout 5

  认证请求如 5 秒没收到应答，将重发该报文。

- was# radius auth port 1812

  配置认证服务的认证端口为 1812。

- was# radius dupacct ip key password

  配置对帐服务器的地址为 202.96.196.2 ，通信密钥为 password。

【注意事项】：

当需要外接 radius 认证时，应该配置认证、计费服务器的地址、通信密钥、端口号，并且要打开 WACS 的认证、计费功能。

比如配置外接 radius 服务器为 192.168.0.111，通信密钥为“ password ”。

- was#radius auth ip 192.168.0.111 key password
- was#radius auth port 1812
- was#radius auth enable
- was#radius acct ip 192.168.0.111 key password
- was#radius acct port 1813
- was#radius acct enable

在和外接 Radius 服务器配合时，要配置正确的认证、计费端口。旧的 Radius 协议定义的认证、计费端口为 1645、1646，而新的 Radius 协议采用的认证、计费端口为 1812、1813。

4.1.24.   radsrv

【用法】：radsrv enable/disable

radsrv debug

【作用】：启用或者禁止本地 Radius 服务

【例如】：

- was #   radsrv   enable

  起用本地 Radius 服务

- was #   radsrv   disable

  禁用本地 Radius 服务，如果本地 Radius 服务正在运行，需要保存配置，重新启动

【注意事项】：

1、 如果本地 Radius 服务已经启动，再禁用本地 Radius 服务，需要保存配置，重新启动设备才能生效。

2、 本地 Radius 使用 1812 和 1813 端口

4.1.25.   reboot

【用法】：reboot

【作用】：重启机器。在改变某些敏感配置（例如端口地址或者端口属性）后或根据需要重新启动服务器。

【例如】：

- was# reboot

  重启机器。

4.1.26.   route

【用法】：route add/del <net> <mask> <gateway>

route show

【作用】：修改、显示路由表。当在网络实际环境使用时，需要加入若干静态路由或者缺省路由到 WACS 中，使报文可以正确到达目的地址。

【例如】：

➢ was#route add 0.0.0.0 0.0.0.0 202.96.196.5

增加缺省静态路由，所有报文都送到下一跳 202.96.196.5。

➢ was#route show

显示系统的路由表状况。

➢ was#route del 0.0.0.0 0.0.0.0 202.96.196.5

删除缺省的静态路由。

4.1.27. servicename

【用法】：servicename <name>

【作用】：定义服务的名称。如果采用外接 Radius 认证计费，则应该和 Radius 服务策略中定义的服务类型结合起来。

【例如】：

➢ was# servicename local

定义服务的名称为 local

➢ was# servicename internet

定义服务的名称为 internet

【参考命令】：aclcfg

【注意事项】：

1、 此命令和计费运营有关，需要特定的外接 Radius 支持

2、 WACS 不推荐使用此命令，使用缺省的配置即可

4.1.28. set

【用法】：set nat_tcptimeout <sec>

set nat_udptimeout <sec>

set nat_icmptimeout <sec>

【作用】：设置某些 nat 活动连接超时参数。

➢ set nat_tcptimeout <sec>

设置 NAT 功能开启后的 tcp 连接的老化时间。

➢ set nat_udptimeout <sec>

设置 NAT 功能开启后的 udp 报文的老化时间。

➢ set nat_icmptimeout <sec>

设置 NAT 功能开启后的 icmp 报文的老化时间。

【例如】：

➢ set nat_tcptimeout 300

设置 NAT 情况下，TCP 报文的老化时间为 300 秒。

➢ set nat_udptimeout 60

设置 NAT 情况下，UDP 报文的老化时间为 60 秒。

➢ set nat_icmptimeout 60

设置 NAT 情况下，ICMP 报文的老化时间为 60 秒。

4.1.29. session

【用法】：session address <begin_ip> <num> [pass]

session echo_timeout <second>

session echo_interval <second>

session acct_interval <minute>

session pass_in_rate <kbits/s>

session pass_out_rate <kbits/s>

session idle_chk enable/disable

session idle_timeout <minute>

session idle_data <kbits>

session max_nat_num <num>

session web_num <num>

【作用】：设置用户连接网络的参数。

➢ session address <begin_ip> <num> [pass]

设置允许接入网络的用户 IP 地址，如果有 pass 参数表示用户访问外网时无需认证。

➢ session echo_timeout <second>

设置页面连接窗口和 WACS 多长时间没有 keepalive 报文交互，就切断其连接，默认时间为 180 秒。

- session echo_interval <second>

  设置 web 认证的连接小窗口和 WACS 之间的 keepalive 报文的交互间隔时间，默认时间 60 秒。

- session acct_interval <minute>

  设置 pass 用户计费报文的发送间隔，默认 60 分钟。如果用户不需要对 Pass 用户进行计费，可以将该参数设置为 0。

- session pass_in_rate <kbits/s>

  设置直通用户的上行速率。

- session pass_out_rate <kbits/s>

  设置直通用户的下行速率。

- session idle_chk enable/disable

  是否开启空闲检查功能。

- session idle_timeout <minute>

  设置空闲检查的时间间隔，默认 5 分钟。

- session idle_data <kbits>

  设置空闲检查的流量信息，默认 3kbits。

- session max_nat_num <num>

  设置用户默认情况下的 NAT 会话量，默认 300 条。

- session web_num <num>

  设置每个用户最多可以发起的 web 认证的连接数，默认 10 个。

【例如】：

- was#session address 10.1.1.2 250

  允许用户使用 10.1.1.2 开始的 250 个 IP 地址进行接入。

- was#session address 10.1.1.220 10 pass

  允许用户使用 10.1.1.220 开始的 10 个 IP 地址无需认证，当这些用户从接入端口访问外网时无需认证，但是外网用户不能主动访问 10.1.1.220 开始的 10 个 IP 地址。

【注意事项】：

因为 session 命令中 session echo_interval/echo_timeout，session idle_chk 这 2 组命令都涉及到 WACS 和用户端（web 认证）之间的 keepalive 报文的交互，影响 WACS 判断

用户异常下线的条件，所以有必要对这 2 组参数之间的关系进行深入的讲解。

A、 session echo_interval/echo_timeout：

当使用 web 认证时，用户端和 WACS 之间 keepalive 报文的发送间隔是 session echo_interval 决定的，当 WACS 在 session echo_timeout 时间内没有收到 keepalive 报文，就会判断用户异常，从而停止用户计费。

B、 session idle_chk enable、session idle_timeout、session idle_data：

当打开 session idle_chk enable 功能时，系统将会对每个用户的流量信息检查。如果在 session idle_timeout 时间内用户的流量没有达到 session idle_data 指定的流量门限，则系统会强制用户下线。

Session idle_chk 功能打开后，如果用户满足 session echo_interval,session echo_timeout 或者 session idle_timeout,session idle_data 这两组条件之一就会被强制下线。

这两组参数之间的关系比较复杂，一定要认真理解它们之间的相互关系，这样才能根据网络情况灵活的进行设置相关参数。

4.1.30. show

【用法】：show <var>

【作用】：显示系统的各种参数。

【例如】：

- was ＃show ?

  列出可以显示的各种系统参数。

- was＃ show config

  显示已配置参数。

4.1.31. snmp

【用法】：snmp com name r|w|rw

snmp trap <ip>

snmp trap_version <num>

【作用】：配置 snmp 协议 community 及读写权限，trap 报文发送的地址和报文的版本号。

【例如】：

- was#snmp com comu1 r

  设置设备 snmp 协议的 community 参数为 comu1，只有读的权限。

- was#snmp com admin rw

  设置设备 snmp 协议的 community 参数为 admin，具有读写的权限。

- was# snmp trap 192.168.0.100

  将 snmp 相关信息发送到管理主机 192.168.0.100。

- was# snmp trap_version 1

  snmp trap 报文按 snmp v1 定义的格式发送。

4.1.32. src_route

【用法】：src_route enable/disable 使能/禁止源地址路由

src_route show 查看源地址路由

src_route add/del <net> <mask> <next_hop>

【作用】：配置源地址路由功能，增加或者删除一条源地址路由配置。增加以后，只要 ip 包的源 ip 落在给定的网络地址掩码范围内，那么不论其它路由配置如何，都把该 ip 包转发给指定的下一跳地址的网关。

【例如】：

- was# src_route enable
- was# src_route add 10.1.2.0 255.255.255.0 192.168.0.3
- was# route add 0.0.0.0 0.0.0.0 192.168.0.2

该命令假设设备上行口 192.168.0.1，有两个上行出口分别是：192.168.0.2 和 192.168.0.3。用户地址段为 10.1.1.0/24 和 10.1.2.0/24，默认路由是 192.168.0.2，而 10.1.2.0 地址段的用户走 192.168.0.3 的路由。

【参考命令】：route

【注意事项】：

1、 此命令适合在有多个子网的环境下使用

2、 WACS 不推荐使用此命令

4.1.33. tcplimit

【用法】：tcplimit　disable/enable/show

tcplimit　default　[num]

tcplimit　user　[ip]

【作用】：对用户的 TCP 连接会话数进行限制，查看用户当前的会话数。

【例如】：

- was#tcplimit enable

  打开 TCP 会话限制功能。

- was#tcplimit default 30

  设置用户默认的所有 TCP 会话连接数为 30。

- was#tcplimit　user 192.168.0.189

  查看 192.168.0.189 当前的会话数。

【注意】：tcplimit user [ip]命令显示的不一定是当前该用户的真实 tcp 连接，因为系统设计时为了减小 cpu 负荷，当用户的 tcp 连接数到达默认的极限时，用户新建的 tcp 连接就会替换原先的处于关闭状态的 tcp 连接。因此当用户实际 tcp 连接数大于或者等于设置的门限值后，tcplimit user [ip]命令看到的不一定是此时用户真实的 tcp 连接状况。

WACS 默认的最大 tcp 连接数可以设置为 30，

当用户打开该功能后，此时用户如果在外接 Radius Server 设置了该用户可以建立的 TCP 连接数，那么该用户认证通过后 Radius Server 返回的参数优先于 WACS 设置的 TCP 连接数。

【注意事项】：

1、 此命令为控制用户使用 TCP 连接数，在页面管理中没有相关控制

2、 在运营商中，此功能比较常用，企业级用户不推荐使用。

4.1.34. telnet

【用法】：telnet ip [port]

【作用】：远程登录指定的主机，可以指定端口。

【例如】：

- was#telnet 192.168.0.189

通过 telnet 登录 192.168.0.189 的设备。

【注意事项】：

1、 此功能为命令行方式特有，在管理页面中无法使用

2、 使用 telnet 主要是方便对大型网络的设备管理

4.1.35. telnetlist

【用法】：telnetlist add/del <ip> <mask>

telnetlist show

【作用】：添加或者删除指定的 ip 子网的主机可以通过 telnet 方式登录 WACS，其他用户不能登录。

【例如】：

- was#telnetlist add 192.168.0.189 255.255.255.255

  允许主机 192.168.0.189 可以 telnet 登录本设备。

- was# telnetlist add 192.168.0.0 255.255.255.0

  允许子网 192.168.0.0 的用户 telnet 登录本设备。

4.1.36. time

【用法】：time [YYYYMMDDHHMM]

【作用】：显示和修改系统时间。

【例如】：

- was#time

  显示系统时间。

- was# time 200012031200

  设置系统时间为 2000 年 12 月 03 日 12 时 00 分。

4.1.37. upgrade

【用法】：upgrade tftp_server file_name

【作用】：通过 tftp server 升级系统。

【例如】：

➢ was# upgrade 202.96.196.3 aos

到 ip 地址为 202.96.196.3 的 tftp server, 下载文件名为 aos 文件作为系统新版本。

【参考命令】：reboot，webadm

【注意事项】：

1、 下载完新版本后，重新启动 WACS 才能启用新的系统

4.1.38. upgrade_lic

【用法】：upgrade_lic tftp_server file_name

【作用】：通过 tftp server 升级系统的 License 信息。

【例如】：

➢ was# upgrade_lic 202.96.196.3 license.lic

到 ip 地址为 202.96.196.3 的 tftp server, 下载文件名为 license.lic 的 License 文件到设备中。

【参考命令】：reboot，show version

【注意事项】：

1、 更新 License 信息后，需要重新启动 WACS 才能生效

4.1.39. user

【用法】：user name <name> passwd <passwd>

【作用】：修改管理用户的密码

【例如】：

➢ was#user name admin passwd pass

修改 admin 的密码为 pass

【参考命令】：enable

【注意事项】：

1、 管理用户只有两个：admin 和 manager

4.1.40. web

【用法】：web put|get tftp_server filename

web ls

web pr filename

web rm filename

【作用】：配置、显示、删除相关 web 认证的文件。要非常谨慎的使用该命令，使用前请和相关的技术支持人员联系。替换掉网页文件后，要执行 webp recache 命令使新的文件生效。

【例如】：

- was#web get 192.168.0.189 cauth.asp

  从 TFTP Server 192.168.0.189 下载 cauth.asp 文件。

- was＃web ls

  显示所有与页面相关的文件。

- was＃web pr cauth.asp

  显示 cauth.asp 文件的内容。

- was＃web rm cauth.asp

  删除 cauth.asp 文件。

【参考命令】：webp，webadm

【注意事项】：

1、 web 命令是对认证的页面进行管理，管理界面的相关命令为 webadm

2、 不要随便替换页面，否则会造成认证不正常

4.1.41. webp

【用法】：webp url <address>

webp pass <ip> <mask>

webp nopass <ip> <mask>

webp vlan_page enable/disable

webp vlan <vlan_id> <num> <portal_file>

webp del vlan <vlan_id> <num>

webp recache

【作用】：设置与 web portal 相关的功能。

- webp url <address>

  指定 web portal，用户认证通过后强制登录指定 url。

- webp pass <ip> <mask>

  指定 IP 可以不用认证进行登录，此时用户访问该 IP 也不会限速和计费。

- webp nopass <ip>

  删除设定的免认证登录 IP。

- webp vlan_page enable/disable

  开启或者关闭 vlan 认证功能。

- webp vlan <vlan_id> <num> <portal_file>

  设置指定 vlan 认证的认证页面文件。

- webp del vlan <vlan_id> <num>

  删除指定 vlan 认证的 vlan ID。

- webp recache

  使上传的页面文件生效。

【例如】：

- was＃webp url http://www.amtium.com

  用户认证后强制登录 www.amtium.com。

- was＃webp url http://0.0.0.0

  取消强制登录指定的 url。

- was＃webp pass 210.10.10.80 255.255.255.255

  访问 210.10.10.80 可以不用认证、不用计费、不用限速。

- was＃webp vlan_page enable

  开启 vlan 认证功能，该功能是提供给酒店上网用，建议 WACS 系列产品不要使用该功能。

- was＃webp vlan_page 110 10 cauth.asp

vlan 110-119 使用 cauth.asp 认证页面进行登录。

- was＃webp del vlan 110 10

  取消 vlan 110 到 vlan 119 的 vlan 认证功能。

【注意事项】：

1、WACS 只使用两 webp pass/nopass/url 这三个功能，其他功能不推荐使用

4.1.42. webadm

【用法】：webadm put|get <tftp_server> <filename>

webadm upgrade <tftp_server>

webadm ls

webadm pr filename

webadm rm filename

webadm online

webadm kick <user>

webadm lang auto|en

【作用】：与管理页面相关的功能设置

- webadm get <tftp server> <filename>

  从 TFTP SERVER 获取某个管理页面文件

- webadm put <tftp server> <filename>

  把某个管理页面文件导出到指定的 TFTP SERVER

- webadm upgrade <tftp server>

  一次性从 TFTP SERVER 获取所有的管理页面，一般用于版本升级中的页面升级

- webadm ls

  显示所有的管理页面文件

- webadm pr filename

  显示指定管理页面文件的内容

- webadm rm filename

  删除指定的页面管理文件，请一定注意，不要随便删除文件。

- webadm online

显示当前已经登录管理页面的管理用户

- webadm kick <user>

  强制已经登录管理页面的管理用户退出，user 参数使用 webadm online 中显示的 ID

- webadm lang auto|en

  管理页面使用英文界面或者自动识别，最好设成自动识别

【例如】：

- was＃webadm get 192.168.0.127 login.asp

  从 192.168.0.127 主机，获取 login.asp 页面

- was＃webadm put 192.168.0.127 login.asp

  把 login.asp 文件导出到 192.168.0.127 上

- was＃webadm upgrade 192.168.0.127

  一次性从 192.168.0.127 上获取系统的所有页面文件

- was＃webadm ls

  显示所有的管理页面文件

- was＃webadm pr login.asp

  显示 login.asp 的文件内容

- was＃webadm rm login.asp

  删除文件 login.asp，删除后不可恢复，管理页面中 login.asp 内容将不可用，谨慎！

- was＃webadm online

  显示当前已经登录管理页面的管理用户

- was＃webadm kick 0

  强制 id 为 0 的管理用户退出管理页面

- was＃webadm lang auto

  管理页面自动识别浏览器的语言，根据识别结果显示中文或者英文界面

4.1.43. wudb

【用法】：wudb put|get <tftp_server> <filename>

wudb del|qry <username>

wudb list|renew|save

【作用】：对本地数据库的用户进行管理，包括导入、导出、删除、查询等操作

【例如】：

- was#wudb get 192.168.1.127 user.txt

从 192.168.1.127 主机上，获取用户文件 user.txt，此文件的内容是用户数据（数据文件格式见附件）

- was#wudb put 192.168.1.127 user.txt

把用户数据导出到主机 192.168.1.127 上保存

- was#wudb qry test1

从用户数据库中查询 test1 用户的内容，显示格式见附件的用户数据文件格式

- was#wudb del test1

从临时用户数据库中删除 test1 的用户，如果要永久删除此用户，需要保存配置

- was#wudb list

显示临时数据库中所有的用户信息，显示格式见附件的用户数据文件格式

- was#wudb renew

把永久数据库中的用户数据同步到临时数据库中

- was#wudb save

把临时数据库中的用户数据保存到永久数据库中

4.1.44. write

【用法】：write

【作用】：存储配置参数到 flash memory 中。

【例如】：

- was# write

将当前配置文件存储到 flash memory。

5. 附件

5.1. dhcp umac 文件格式

dhcp umac 使用的文件为文本格式，可以通过 TFTP 工具上传到 WACS。

文件格式定义如下：

IP1　　MAC1

IP2　　MAC2

……

IPn　　MACn

其中 IP 的格式为：

nnn . nnn . nnn . nnn

MAC 的格式为：

mm : mm : mm : mm : mm : mm

例如：

192.168.1.61　　00:03:47:3C:98:11

192.168.1.62　　00:03:47:3C:98:12

192.168.1.63　　00:03:47:3C:98:13

192.168.1.64　　00:03:47:3C:98:14

5.2. 用户数据文件格式

以空格分隔

name|password|ip|bindip|mac|bind_mac|vlan|bind_vlan|up_rate|down_rate|online_max|enabled|start Date|expired Date|

字段名	字段含义
name	帐号名
password	密码
ip	用户的 IP
bindip	是否绑定 IP
mac	用户的 MAC
bind_mac	是否绑定 MAC
vlan	用户的 VLAN
bind_vlan	是否绑定 VLAN
up_rate	上行速率
down_rate	下行速率
online_max	最大在线用户
enabled	是否有效
Start Date	生效日期（整数，从 1970-01-01 00:00:00 开始算起的秒数）

Expired Date	失效日期（整数，从 1970-01-01 00:00:00 开始算起的秒数）

5.3. 如果正确升级版本

WACS 的版本升级包括两个方面：
1、 操作系统的升级
2、 管理页面升级

升级版本有两种方式：用命令行或者页面进行升级。

如果采用命令行方式，正确的操作步骤如下：
1、 用串行线连接到 wacs，或者直接 telnet 到 wacs，输入用户名/密码，登录
2、 运行 enable 命令，输入 enable 的密码（缺省为 eflow），进入配置模式
3、 先用 upgrade 命令把新版本软件下载到 WACS 设备（详细命令请看 upgrade 命令）
4、 重新启动 WACS，让新版本操作系统生效
5、 重复 1、2 两步骤
6、 用 webadm upgrade 把新的管理页面下载过来
7、 再重新启动设备
8、 升级完成

如果采用页面方式升级，操作步骤如下：
1、 打开浏览器，用 admin 用户登录进去
2、 到“系统管理”的“版本升级”界面
3、 先升级系统，输入 tftp 服务器地址和系统的文件名，点确定
4、 升级完成，到“系统管理”的“重新启动”界面，选择不保存配置重新启动
5、 重复 1、2 两步骤
6、 输入 tftp 服务器地址，升级页面
7、 升级完成，到“系统管理”的“重新启动”界面，选择不保存配置重新启动
8、 升级结束

需要注意的地方：
1、 页面是多个文件组成，在升级页面前，需要在 tftp 服务器建立一个目录，把页面文件放在此目录下，tftp 服务器的根目录指向此目录
2、 升级完成，需要重新启动才能把新系统运行起来

5.4. 如何获取新的 License 文件并进行更新

设备的 License 是对同时上网的用户数进行控制。如果正在使用的设备，需要增加同时上网的用户数，可以采用更新 License 的办法来实现。

对 License 进行更新可以采用页面或者命令行的方式进行。

如果采用命令行方式，步骤如下：
1、 找出设备的序列号，联系对应的技术支持或者销售，获取新的 License 文件
2、 用串行线连接到 wacs，或者直接 telnet 到 wacs，输入用户名/密码，登录
3、 运行 enable 命令，输入 enable 的密码（缺省为 eflow），进入配置模式
4、 运行 upgrade_lic 命令，把 license 文件下载到设备上
5、 重新启动设备
6、 设备启动后，登录进入，用 show version 命令查看新的 License 是否生效

如果采用页面方式，操作步骤如下：
1、 找出设备的序列号，联系对应的技术支持或者销售，获取新的 License 文件
2、 打开浏览器，用 admin 用户登录进去
3、 到“ 系统管理 ”的“ 版本升级 ”界面
4、 升级用户 License
5、 到“ 系统管理 ”的“ 重新启动 ”界面，选择不保存配置重新启动
6、 重复 1、2 两步
7、 到“ 系统管理 ”的“ 查看状态 ”中，查看系统版本信息是否已经更新

5.5. 为什么使用过程中会经常出现需要认证的页面？

当 WACS 作为认证点，或者放在出口作为网关使用时会出现这种情况。

造成这种现象的原因如下：

当采用 web 认证时，在认证通过后，WACS 会在用户的机器上推出一个小的浏览器窗口，这个小窗口每隔一定的时间（参看《WACS 用户手册》的“ 认证管理 ”的“ web 认证管理 ”界面，或者《WACS 高级用户手册》的 session 命令），会采用随机的算法，和 WACS 进行一次通信，以避免有人抢占已认证用户的 IP 上网。这就是 WACS 中的 Keep-alive 机制。

WACS 会定时检查用户通信的时间，如果超出定义的时间，未收到小窗口发送过来的 Keep-alive 数据，WACS 即认为此用户已经不在线，把此用户从在线用户中删除。

很多浏览器安装了上网助手或者防火墙之类的软件，会拦截浏览器的弹出窗口，这样，用户就不会看到认证后的小浏览器窗口，造成 Keep-alive 机制不能正常进行。在 Keep-alive 超时时间（缺省为 3600 秒）一过，用户就需要重新认证才能上网。

如何解决这个问题：

针对这种问题，在网络环境比较固定，地址冲突情况比较少的企业环境中，可以采用流量检查的方式来避免。（参看《WACS 用户手册》的“ 认证管理 ”的“ web 认证管理 ”界面，或者《WACS 高级用户手册》的 session 命令，和 idle-timeout 或者 idle_chk 相关的参数）

首先，把 Keep-alive 的 timeout 时间设置为很大，比如 10 个小时（36000），避免 Keep-alive 超时。

然后，打开 idle-timeout 的检查，定义 idle 检查的流量和时间间隔，当用户在此时间流量未超过此界限，即认为用户已经下线。

如果对网内安全比较重视，建议用户最好能关闭浏览器对弹出窗口的拦截，正常启用

Keep-alive 的检查机制。（参看 IE 浏览器的“ 工具 ”菜单）

5.6. 采用 DHCP 分配地址，为什么会出现地址冲突？

出现地址冲突有两个原因：

1、 有用户直接在网络设置中手动输入地址

2、 DHCP 检查机制不能正常运作

对于第一种情况，只能让网络管理员进行提醒和排查。

对于第二种情况，原因和解决办法如下：

WACS 的 DHCP 在分配地址前，采用 ICMP 包检查是否此地址是否会使用，有些机器安装了个人防火墙，对发给本机的 ICMP 数据不会做出回应，所以会导致 DHCP 的检查机制不能正常运作。

针对这种情况，最好能在个人防火墙打开此限制，或者设置规则，允许 wacs 向用户机器发送 ICMP 包。

5.7. 设置 ACL 规则，怎么不起作用？

ACL 规则请参看《WACS 高级用户手册》的 filist 命令，或者《WACS 用户手册》的“ 高级配置 ”中“ ACL 配置 ”界面。

在 WACS 的 ACL 规则中，针对端口（WAN、LAN、DMZ、WANppp0），定义了 in 和 out，也就是数据包的进出方向。

如果用户在 LAN 端口下，用户发给外面的数据，对 LAN 端口就是 in，外面返回给用户的数据，对 LAN 端口就是 out。

同样，用户发送出去的数据，对 WAN 端口就是 out，外面返回给用户的数据，对 WAN 就是 in。

在制定规则前，需要仔细考虑数据的进出方向。

例如：

LAN 端口地址配置为 10.1.1.1/255.255.255.0

WAN 端口地址配置为 192.168.0.2/255.255.255.0

企业内部网络的服务器地址在 192.168.0.0/24 这一网段，用户需要能 ping 通内部的所有地址，但是不允许 ping 其他的地址，规则设置如下：

block	LAN	in	icmp	10.1.1.0/24	0.0.0.0/0	继续
pass	LAN	in	icmp	10.1.1.0/24	192.168.0.0/24	返回

5.8. 管理页面不能打开，如何查看和对机器进行配置？

如果管理页面异常，可以通过命令行方式查看设备的配置。命令行的命令解释请查看《WACS 高级用户手册》

进入命令行的方式有两中：通过串口或者 telnet 方式。

如果采用 telnet：

1、 先把管理机器的 IP 配置和 WACS 的 WAN 端口或者 DMZ 端口在同一网段，然后在 Windows 下运行 telnet 命令
2、 输入用户名和密码（admin 或者 manager 用户，密码缺省为 password）
3、 如果需要进行配置，在登录进去后，运行 enable 命令，输入 enable 密码，缺省为 eflow
4、 运行 show config 可以查看当前的所有配置，或者运行 show，会给出可以查看哪些配置的提示
5、 输入?，会提示可以使用哪些命令
6、 直接输入命令名字，然后回车，可以看到此命令的用法

如果忘记了 WACS 的端口地址，或者地址已经不可用，可以从串口登录查看配置：

1、 用随机附带的串行线连接管理机器的串口和 WACS 的 console 口（连接 WACS 上面位置的 console 口）
2、 在 windows 下，打开超级终端（参数设置：每秒位数-9600 数据位-8 奇偶校验-无 停止位-1 数据流控制-Xon/Xoff），回车，会出现登录提示
3、 输入用户名和密码（admin 和 manager，缺省密码为 password）
4、 其他步骤见上面 telnet 方式的 3~6 步

5.9. 机器重新启动后，不需要认证就可以上网？

WACS 采用了 Keep-alive 的检查机制（具体参看附件 5.4 中的描述）。

如果用户没有正常申请下线（点击弹出小窗口中的退出），直接重新启动机器，当机器正常启动后，其中的时间间隔还没有超过 Keep-alive 的超时时间。在这种情况下，WACS 设备认为用户还是正常在线，因此可以直接上网。

如果用户采用了正常的下线方式，不会出现这种情况。

即使用户可以直接上网，由于没有 Keep-alive 机制保证，在超时时间一过，还是需要重新认证。如果用户不想在上网中被迫重新认证，在出现这种情况时，请联系管理员，强制删除在线表中的用户，然后，采用正常的认证过程上网。